UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/617,258	07/11/2003	Ihab Hamadeh	59516-042	2408

7590 08/19/2009

MCDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
SMARTH, GERALD A	

ART UNIT	PAPER NUMBER
2446	

MAIL DATE	DELIVERY MODE
08/19/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/617,258	HAMADEH ET AL.	
	Examiner	Art Unit	
	GERALD SMARTH	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/27/04, 07/11/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/617258 has a total of 41 claims pending in the application; there are 7 independent claims and 34 dependent claims, all of which are ready for examination by the examiner.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 31-41 are rejected under 35 U.S.C. 102(e) as being unpatentable by Munger (2002/0161925),

Regarding claim 34, Munger teaches a computer system configured to implement a sequence of steps, to identify a device at or near a point of origin of a particular flow of packets through a packet data communication network, ***(Munger discloses FIG. 14 shows a "checkpoint" scheme for regaining synchronization between a sender***

and recipient; Paragraph 42) the sequence of steps comprising: receiving data packets containing marks comprising fragments of a network address of the device, via the packet data communication network; ***(Munger discloses After encryption, the encrypted block is broken into separate payloads and segments which are interleaved as in the embodiment of FIG. 3a. The resulting interleaved packets A, B, and C, are then packaged as TARP packets with TARP headers as in the Example of FIG. 3a; paragraph 78 lines 11-15)*** for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets to determine if there is a match; ***(Munger discloses When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set; Paragraph 124 lines 1-4)*** and for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments, wherein the matching and concatenation is performed one or more times until a combination of fragments produces a complete address of a device that marked a plurality of the received packets. ***(Munger discloses the session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed; paragraph 13 lines 4-6)***

Regarding claim 35, Munger teaches a computer program product comprising executable code embodied in a machine-readable medium, execution of the code causing a computer to perform a sequence of steps to identify a device at or near a point of origin of a particular flow of packets through the network, the sequence of steps comprising: receiving data packets containing marks comprising fragments of a network address, via the packet data communication network; (***Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:; Paragraph 68 lines 9-14)*** for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets to determine if there is a match; and for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, ***(Munger discloses When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set; Paragraph 124 lines 1-4)*** concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments, wherein the matching and concatenation is performed one or more times until a combination of fragments produces a complete address of a device that marked a plurality of the received packets. ***(Munger discloses***

the session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed; Paragraph 65 lines 7-9)

Regarding claim 36, Munger teaches a method of marking communication packets forwarded by a router through a packet data communication network with router identifying information, comprising: ***(Munger discloses FIG. 16 shows how two addressees adresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)*** forming one or more first fragments from a first network address associated with the router; forming one or more second fragments from a second network address associated with the router; and marking a plurality of packets by adding the fragments to the plurality of packets; and forwarding the plurality of marked packets from the router through the packet data communication network. ***(Munger discloses the session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed; Paragraph 65 lines 7-9)***

Regarding claim 37, Munger taught the method of claim 36, as described above. Mugner further wherein the first and second addresses are Internet Protocol (IP) addresses of the router. ***(Munger discloses When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set; Paragraph 124 lines 1-4)***

Regarding claim 38, Munger taught the method of claim 36, as described above. Munger further teaches wherein at least one of the first and second network addresses is scrambled before the step of forming one or more fragments thereof. ***(Munger discloses each packet destined for a low-bandwidth node is cryptographically authenticated to determine whether it belongs to a VPN; Paragraph 239 lines 5-9)***

Regarding claim 39, Munger taught the method of claim 36, as described above. Munger further teaches wherein the first address comprises an Internet Protocol (IP) address of the router and the second address comprises a scrambled IP address of the router. ***(Munger discloses the session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed; Paragraph 65 lines 7-9)***

Regarding claim 40, Munger taught the method of claim 36, as described above. Munger furhter teaches wherein: the first network address is scrambled before the step of forming one or more fragments thereof; and the second network address is hashed network address is before the step of forming one or more fragments thereof. ***(Munger teaches one implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value; Paragraph 168 lines 1-4)***

Regarding claim 41, Munger taught the method of claim 36, as described above. Munger further teaches wherein the forming steps produce fragments of one or more Internet Protocol (IP) addresses, fragments of one or more scrambled IP addresses and fragments of one or more hashed IP addresses. ***(Munger teaches one implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value; Paragraph 168 lines 1-4)***

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 1-30 rejected under 35 U.S.C. 103(a) as being unpatentable over Munger (2002/0161925) in view of Poletto (2003/0145232),

Regarding claim 1, Munger teaches a method for enabling identification of at least one address associated with ingress of a packet stream, comprising: identifying a portion of a packet data communication network as a trusted region; identifying all border devices

at entry points on an outer boundary of the trusted region of the network; ***(Poletto discloses the gateway 26 devices are located at the edges of the Internet 14, for instance, at the entry points of data centers. The gateway devices constantly analyze traffic, looking for congestion or traffic levels that indicate the onset of a Dos attack.; paragraph 27 lines 9-13)*** configuring each respective one of the border devices to mark at least predetermined packets transmitted into the trusted region of the network, ***(Munger discloses special TARP headers IP.sub.T are then added to each payload using IP headers from the data stream packets; Paragraph 15)***each marking of a packet by a respective border device comprising providing a fragment of a network address of the respective border device with the packet; receiving a plurality of marked packets from one of the border devices; and processing address fragments from the received marked packets to reconstruct the network address of the one border device. ***(Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers: Paragraph 68 lines 9-14)***

Munger does not explicitly disclose identifying all border devices at entry points on an outer boundary of the trusted region of the network.

However Poletto does teach identifying all border devices at entry points on an outer boundary of the trusted region of the network.

It would be obvious to a person of ordinary skill in the art at the time of the invention to modify an agile network protocol for secure communcaitons with assured system

availability of Munger to add a Denial of service attacks characterization of Poletto. One of ordinary skill in the art would have been motivated to make this modification in order to have a system which can be more robust for detection denial of service attacks. *Poletto discloses aspects of the invention provide a technique to detect and determine packets that are part of a denial of service attack. The technique can protect links between the Internet and an attacked data center as well as devices within the data center. In one embodiment, a gateway device is deployed physically in line. The gateway device includes a filter process to decide whether to forward network traffic based on values of the examined attributes. The gateway filters detected malicious traffic by discarding packets that the gateway deems to be part of an attack; Paragraph 009.*

Therefore, it would be obvious to combine Munger and Poletto to arrive at the limitations in claim 1.

Regarding claim 2, Munger in view of Poletto taught the method of claim 1, as described above. Poletto teaches wherein the configuring step comprises causing each respective border device to mark all packets being transmitted into the trusted region of the network. ***(Poletto discloses the gateway 26 devices are located at the edges of the Internet 14, for instance, at the entry points of data centers. The gateway devices constantly analyze traffic, looking for congestion or traffic levels that indicate the onset of a Dos attack.; paragraph 27 lines 9-13)***

Regarding claim 3, Munger in view of Poletto taught the method of claim 1, as described above. wherein the configuring step comprises causing each respective border device to mark all packets being transmitted to a predetermined destination through a region of the network trusted by the predetermined destination. ***(Munger discloses special TARP headers IP.sub.T are then added to each payload using IP headers from the data stream packets; Paragraph 15)***

Regarding claim 4, Munger in view of Poletto taught the method of claim 1, as described above. Munger further teaches wherein the identified border devices comprise a plurality of routers of one or more autonomous systems of the packet data communication network. ***(Munger discloses FIG. 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table; Paragraph 129 lines 34-37)***

Regarding claim 5, Munger in view of Poletto taught the method of claim 4, as described above. Munger further teaches wherein the packet data communication network is the Internet. ***(Poletto discloses a plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses; Abstract)***

Regarding claim 6, Munger in view of Poletto taught the method of claim 4, as

described above. Munger further teaches wherein the plurality of routers include routers on a backbone of one or more autonomous systems. ***(Munger discloses A secure mechanism for communicating over the internet, including a protocol referred to as the Tunneled Agile Routing Protocol (TARP), uses a unique two-layer encryption format and special TARP routers.; Paragraph 9 lines 1-3)***

Regarding claim 7, Munger in view of Poletto taught the method of claim 1, as described above. Munger further teaches wherein each respective one of the configured border devices performs the following steps: fragmenting an address of the respective border device into a first plurality of overlapping fragments of a first format; ***(Munger discloses FIG. 16 shows how two addressees adresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)*** assigning fragment identifiers of a first range to the first fragments; fragmenting the address of the respective border device into a second plurality of overlapping fragments of a second format; ***(Munger discloses FIG. 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table; Paragraph 129 lines 34-37)***assigning fragment identifiers of a second range to the second fragments; and marking a plurality of packets forwarded therefrom into the trusted region by adding the first and second fragments and corresponding assigned identifiers to the plurality of packets forwarded by the

respective border device. ***(Munger discloses special TARP headers IP.sub.T are then added to each payload using IP headers from the data stream packets; Paragraph 15)***

Regarding claim 8, Munger in view of Poletto taught the method of claim 7, as described above. Munger in view wherein: the first fragments are formatted to comprise sequential sections of the address of the respective border device having a predetermined number of bits of overlap between consecutive ones of the sequential sections; ***(Munger discloses FIG. 16 shows how two addressees adresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)*** and the second fragments are formatted so that each second fragment comprises two offset sections of the address of the respective border device, at least one pair of the second fragments having a predetermined number of bits of overlap. ***(Munger discloses FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)***

Regarding claim 9. Munger in view of Poletto taught the method of claim 7, as described above. Munger further teaches wherein the step of processing address fragments from the received marked packets to reconstruct the network address of the one border device comprises: processing fragments from said plurality of packets forwarded by the border device having identifiers in the first range to compare overlapped bits and combine fragments having matching overlapping bits to a form first

copy of the address of the one border device from the first fragments; ***(Poletto discloses unusual amounts of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets; Paragraph 76)*** processing fragments from said plurality of packets forwarded by the border device having identifiers in the second range to compare overlapped bits and combine fragments having matching overlapping bits to form a second copy of the address of the one border device from the first fragments; and recognizing a valid reconstructed address if the first and second copies of the address of the one border device match. ***(Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers: Paragraph 68 lines 9-14)***

Regarding claim 10, Munger in view of Poletto taught the method of claim 1, as described above. Munger further teaches wherein the predetermined packets include packets of a type selected from the group consisting essentially of: packets relating to a denial of service attack; packets containing spam e-mail messages; high volume traffic and packets containing illegally distributed content. ***(Munger discloses Each node executes one or more application programs 1203 and 1218 that communicate by transmitting packets through communication software 1204 and 1217, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like; Page 9***

paragraph 140 lines 3-8)

Regarding claim 11, Munger in view of Poletto taught the method of claim 1, as described above. Munger teaches in combination with at least one step for imposing control on a flow of packets through the one border device whose network address was reconstructed from fragments in received packets. ***(Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers: Paragraph 68 lines 9-14)***

Regarding claim 12, Munger in view of Poletto taught the method of claim 10, as described above. Munger teaches wherein the at least one step of imposing control comprises causing the one border device to block transmission into the trusted region of the network of packets addressed to a predetermined destination. ***(Poletto discloses If the attacker is behind a gateway 26, the control center issues a request to the appropriate gateway 26 to block the attacking traffic, e.g. by allowing the appropriate gateway 26 to discard traffic, e.g., packets that contain the victim 12 destination address; Paragraph 47 lines 3-8)***

Regarding claim 13, Munger in view of Poletto taught the method of claim 1, as described above. Munger further teaches wherein packet data communication network

transports Internet Protocol (IP) type packets comprising headers and data, and each marking of a packet comprises inserting the fragment of the network address of the respective border device into a predetermined field of the IP header of the marked packet. ***(Munger discloses to that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 1210X to generate source and destination hardware addresses that are inserted into frame headers(e.g., fields 1101A and 1101B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202; Paragraph 150 lines 5-10)***

Regarding claim 14, Munger in view of Poletto taught the method of claim 13, as described above. Poletto also teaches wherein the predetermined field comprises the Fragmentation Offset field of the IP header. ***(Poletto discloses unusual amounts of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets; Paragraph 76)***

Regarding claim 15, Munger in view of Poletto taught the method of claim 13, as described above. Munger further teaches wherein the predetermined field comprises the Identification field of the IP header. ***(Munger discloses to that end, node 1201 further maintains a transmit table 1210 using a transmit algorithm 1210X to generate source and destination hardware addresses that are inserted into frame headers(e.g., fields 1101A and 1101B in FIG. 11) that are synchronized to a corresponding receive table 1224 at node 1202; Paragraph 150 lines 5-10)***

Regarding claim 16, Munger in view of Poletto taught the method of claim 13, wherein the predetermined field comprises the Fragmentation Offset field and the Identification field of the IP header. ***(Poletto discloses unusual amounts of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets; Paragraph 76)***

Regarding claim 17, Munger in view of Poletto taught the method of claim 16, wherein the fragments comprise IP addresses. ***(Poletto discloses unusual amounts of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets; Paragraph 76)***

Regarding claim 18, Munger teaches a method of marking communication packets forwarded by a router through a packet data communication network with router identifying information, comprising: fragmenting a network address of the router into a first plurality of overlapping address fragments of a first format; ***(Munger discloses FIG. 16 shows how two addressees adresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)*** assigning fragment identifiers of a first range to the first fragments; fragmenting the network address of the router into a second plurality of overlapping address fragments of a second format; ***(Poletto discloses unusual amounts of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets; Paragraph 76)*** assigning fragment identifiers of a second range to the second fragments; and adding

the fragments and corresponding assigned identifiers to a plurality of packets forwarded by the router. ***(Munger discloses special TARP headers IP.sub.T are then added to each payload using IP headers from the data stream packets; Paragraph 15)***

Munger does not explicitly disclose fragmenting the network address of the router into a second plurality of overlapping address fragments of a second format.

However Poletto does teach fragmenting the network address of the router into a second plurality of overlapping address fragments of a second format.

It would be obvious to a person of ordinary skill in the art at the time of the invention to modify an agile network protocol for secure communcaitons with assured system availability of Munger to add a Denial of service attacks characterization of Poletto. One of ordinary skill in the art would have been motivated to make this modification in order to have a system which can be more robust for detection denial of service attacks. *Poletto discloses aspects of the invention provide a technique to detect and determine packets that are part of a denial of service attack. The technique can protect links between the Internet and an attacked data center as well as devices within the data center. In one embodiment, a gateway device is deployed physically in line. The gateway device includes a filter process to decide whether to forward network traffic based on values of the examined attributes. The gateway filters detected malicious traffic by discarding packets that the gateway deems to be part of an attack; Paragraph 009.*

Therefore, it would be obvious to combine Munger and Poletto to arrive at the limitations in claim 18.

Regarding claim 19, Munger in view of Poletto taught the method of claim 18, as described above. Munger teaches wherein: the first address fragments are formatted to comprise sequential sections of the network address of the router having a predetermined number of bits of overlap between consecutive ones of the sequential sections; ***(Munger discloses FIG. 16 shows how two addressees adresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)*** and the second address fragments are formatted so that each second address fragment comprises two offset sections of the address of the router, at least one pair of the second address fragments having a predetermined number of bits of overlap. ***(Munger discloses Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm; Paragraph 25 lines 9-16)***

Regarding claim 20, Munger in view of Poletto taught the method of claim 18, as described above. Munger teaches further comprising forming a hash value from each respective fragment, wherein when each respective fragment is added to a particular packet the hash value formed from the respective fragment is also added to the particular packet. ***(Munger teaches one implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value; Paragraph 168 lines 1-4)***

Regarding claim 21, A method of reconstructing an address of a marking device connected at a point on a packet data communication network at or near a source of a flow of packets through the network, comprising: receiving data packets of the flow containing marks comprising fragments of a network address of the marking device, via the packet data communication network;***(Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers:; Paragraph 68 lines 9-14)*** for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets, to determine if there is a match; ***(Poletto discloses One mechanism compares each parameter (field in a packet) to a list of suspicious values for that parameter, and drops packets for which matches occur; Paragraph 111)***and for each match between a respective fragment from a newly received packet and a fragment from a previously received packet, concatenating one of the matching fragments with non-matched bits of the other one of the matching fragments, ***(Munger discloses When the router receives the client's packet, it compares the send and receive IP addresses of the packet with the next N predicted send and receive IP address pairs and rejects the packet if it is not a member of this set; Paragraph 124 lines 1-4)*** wherein the matching and concatenation is performed one or more times until a

combination of fragments produces a complete address of the device that marked a plurality of the received packets of the flow. ***(Munger discloses the session key is used to decrypt the payloads of the TARP packets 140 permitting an entire message to be reconstructed; Paragraph 65 lines 7-9)***

Munger does not explicitly teach for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets, to determine if there is a match;.

However Poletto does teach for each respective fragment from a newly received packet, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets, to determine if there is a match;.

It would be obvious to a person of ordinary skill in the art at the time of the invention to modify an agile network protocol for secure communcaitons with assured system availability of Munger to add a Denial of service attacks characterization of Poletto. One of ordinary skill in the art would have been motivated to make this modification in order to have a system which can be more robust for detection denial of service attacks. *Poletto discloses aspects of the invention provide a technique to detect and determine packets that are part of a denial of service attack. The technique can protect links between the Internet and an attacked data center as well as devices within the data center. In one embodiment, a gateway device is deployed physically in line. The gateway device includes a filter process to decide whether to forward network traffic*

based on values of the examined attributes. The gateway filters detected malicious traffic by discarding packets that the gateway deems to be part of an attack; Paragraph 009.

Therefore, it would be obvious to combine Munger and Poletto to arrive at the limitations in claim 21.

Regarding claim 22, Munger in view of Poletto taught the method of claim 21, as described above. Poletto teaches wherein the complete address is an Internet Protocol (IP) address of a router on a border of a trusted region of the packet data communication network. ***(Poletto discloses a plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses; Abstract)***

Regarding claim 23, Munger in view of Poletto taught the method of claim 22, as described above. Poletto teaches wherein the packet data communication network is the Internet. ***(Poletto discloses a plurality of computer nodes communicate using seemingly random Internet Protocol source and destination addresses; Abstract)***

Regarding claim 24, Munger in view of Poletto taught the method of claim 23, as described above. wherein the complete address identifies an ingress point of the flow of packets representing an attack on at least one target served through the trusted

region. ***(Poletto discloses the gateway 26 devices are located at the edges of the Internet 14, for instance, at the entry points of data centers. The gateway devices constantly analyze traffic, looking for congestion or traffic levels that indicate the onset of a Dos attack.; paragraph 27 lines 9-13)***

Regarding claim 25, Munger in view of Poletto taught the method of claim 23, as described above. Munger teaches wherein the complete address identifies an ingress point of a flow of packets containing spam e-mails. ***(Munger discloses Each node executes one or more application programs 1203 and 1218 that communicate by transmitting packets through communication software 1204 and 1217, respectively. Examples of application programs include video conferencing, e-mail, word processing programs, telephony, and the like; Page 9 paragraph 140 lines 3-8)***

Regarding claim 26, Munger in view of Poletto taught the method of claim 23, as described above. Munger teaches wherein the complete address identifies an ingress point of a flow of packets containing illegal information content. ***(Munger teaches a large-to-small link bandwidth management feature that prevents denial-of-service attacks at system chokepoints; Paragraph 226 lines 7-9)***

Regarding claim 27, Munger in view of Poletto taught the method of claim 21, as

described above. wherein: the received data packets contain respective fragment identifiers, in first and second ranges; the matching and concatenation is performed on fragments assigned identifiers in the first range and produces a first version of the complete address; ***(Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers: Paragraph 68 lines 9-14)***the method further comprises: for each respective fragment from a newly received packet containing a fragment identifier in the second range***(Munger discloses FIG. 9; the intra-LAN TARP nodes transmit table will be identical to the border node's receive table, and the intra-LAN TARP node's receive table will be identical to the border node's transmit table; Paragraph 129 lines 34-3)***, comparing predetermined bits of the respective fragment to predetermined bits of one or more fragments from previously received packets carrying identifiers in the second range, to determine if there is a match; ***(Munger discloses FIG. 16 shows how two addresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)*** and for each match between a respective fragment from a newly received packet containing a fragment identifier in the second range and a fragment from a previously received packet containing a fragment identifier in the second range, concatenating one of the matching fragments with non-matched bits the other one of the matching fragments, wherein the matching and concatenation for fragments from packets containing fragment identifiers in the second range is performed

one or more times until a combination of fragments produces a second version of the complete address of the device that marked a plurality of the received packets. ***(Munger discloses Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm; Paragraph 25 lines 9-16)***

Regarding claim 28, Munger in view of Poletto taught the method of claim 27, as described above. Munger also teaches further comprising validating the complete address if the first version and the second version match. ***(Munger discloses FIG. 16 shows how two addressees adresses can be decomposed into a plurality of segments for comparison with presence vectors; Paragraph 42)***

Regarding claim 29, Munger in view of Poletto taught the method of claim 21, as described above. further comprising: for each received data packet containing a mark, recovering and storing a hash value related to a respective mark from the received data packet containing the respective mark; upon deriving the complete address, examining stored hash values corresponding to fragments used to derive the complete address; ***(Munger teaches one implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value; Paragraph 168 lines 1-4)***and identifying the complete address as relating to a source of an attack if at least a predetermined number of hash values

corresponding to fragments used to derive the complete address have been received and stored. ***(Poletto discloses If the attacker is behind a gateway 26, the control center issues a request to the appropriate gateway 26 to block the attacking traffic, e.g. by allowing the appropriate gateway 26 to discard traffic, e.g., packets that contain the victim 12 destination address; Paragraph 47 lines 3-8)***

Regarding claim 30, Munger in view of Poletto taught the method of claim 29, as described above. Munger teaches wherein the step of examining comprises: forming a hash of the complete address; fragmenting the hash of the complete address; and comparing the hash fragments to the stored hash values corresponding to fragments used to derive the complete address. ***(Munger teaches one implementation of this is to use a hashing function with a one-to-one mapping to generate the private and public sync portions from the sync value; Paragraph 168 lines 1-4)***

Regarding claim 31, Munger teaches a border device for communication through a packet data communication network, comprising: a communication interface for enabling transmission of packets through the packet data communication network; ***(Munger discloses as shown in FIG. 21, computer 2001 or edge router 2003 incorporates a plurality of link transmission tables 2100 that identify, for each potential transmission path through the network, valid sets of IP addresses that can be used to transmit the packet Paragraph 225 lines 1-4) ;*** and means for

marking at least predetermined ones of the packets transmitted through the packet data communication network, wherein marking operations performed by said means comprise: a) fragmenting a network address of the border device into a first plurality of overlapping fragments of a first format; ***(Poletto discloses unusual amounts of IP fragmentation, or fragmented IP packets with bad or overlapping fragment offsets; Paragraph 76)*** b) assigning fragment identifiers of a first range to the first fragments; c) fragmenting the network address of the border device into a second plurality of overlapping fragments of a second format; ***(Munger discloses Overlapping or "reusable" IP addresses may be allocated to different users on the same subnet, since each node merely verifies that a particular packet includes a valid source/destination pair from the agreed-upon algorithm. Source/destination pairs are preferably not reused between any two nodes during any given end-to-end session, though limited IP block sizes or lengthy sessions might require it; Paragraph 23 lines 9-16)*** d) assigning fragment identifiers of a second range to the second fragments; ***(Munger discloses In a preferred embodiment, the TARP headers IP.sub.T are IP headers with added data providing the following information required for routing and reconstruction of messages, some of which data is ordinarily, or capable of being, contained in normal IP headers: Paragraph 68 lines 9-14)***e) adding the fragments and corresponding assigned identifiers to at least the predetermined ones of the packets transmitted through packet data communication network. ***(Munger discloses special TARP headers IP.sub.T are then added to each payload using IP headers from the data stream packets; Paragraph 15)***

Munger does not explicitly fragmenting a network address of the border device into a first plurality of overlapping fragments of a first format.

However Poletto does teach fragmenting a network address of the border device into a first plurality of overlapping fragments of a first format.

It would be obvious to a person of ordinary skill in the art at the time of the invention to modify an agile network protocol for secure communcaitons with assured system availability of Munger to add a Denial of service attacks characterization of Poletto. One of ordinary skill in the art would have been motivated to make this modification in order to have a system which can be more robust for detection denial of service attacks. *Poletto discloses aspects of the invention provide a technique to detect and determine packets that are part of a denial of service attack. The technique can protect links between the Internet and an attacked data center as well as devices within the data center. In one embodiment, a gateway device is deployed physically in line. The gateway device includes a filter process to decide whether to forward network traffic based on values of the examined attributes. The gateway filters detected malicious traffic by discarding packets that the gateway deems to be part of an attack; Paragraph 009.*

Therefore, it would be obvious to combine Munger and Poletto to arrive at the limitations in claim 31.

Regarding claim 32, Munger in view of Poletto further taught the border device as in claim 31, as described above. Munger further teaches wherein the border device is a

router, and the means for marking comprise an input port processor in a line card of the router. ***(Munger further teaches in one variant of this embodiment, the network includes two edge routers 2003 and 2004 each of which is linked to a plurality of Internet Service Providers (ISPs) 2005 through 2010; Paragraph 224 lines 4-7)***

Regarding claim 33, Munger in view of Poletto further taught the border device as in claim 31, as described above. Munger further teaches wherein the border device is a router, and the means for marking includes a content addressable memory for use in determining if individual packets should be marked. ***(Munger discloses special TARP headers IP.sub.T are then added to each payload using IP headers from the data stream packets; Paragraph 15)***

Conclusion

6. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05 ©.

7. The following reference teaches execution of trial data.

US 2003/0036970

US 2003/0035370

US 7188366

US 7215637

US 6834310

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claim. That is indicated support for newly added claim language by specifically pointing to page(s) and line no(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Gerald Smarth whose telephone number is (571)270-1923. The examiner can normally be reached on Monday-Friday(7:30am-5:00pm)est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on (571)272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Gerald Smarth/

Examiner, Art Unit 2446

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446